

From Phishing To Advanced Persistent Threats: The Application Of Cybercrime Risk To The Enterprise Risk Management Model

John W. Moore, Virginia State University, USA

ABSTRACT

This paper examines the issues of cybercrime in the context of risk to organizations. In particular, it considers the control frameworks most commonly used by U.S. public companies to benchmark their internal controls over financial reporting. It discusses the market for stolen identities, looking at the sources from which many of those identities are stolen. It reviews the available internal control frameworks and explains how a firm's risk of cybercrime might be classified as a material weakness under Sarbanes-Oxley Section 404. It models how the use of COSO's Enterprise Risk Management model could improve an organization's chances of avoiding a serious incident.

Keywords: cybercrime; internal control frameworks; Sarbanes Oxley Section 404; material weaknesses

INTRODUCTION

Cybercrimes aimed at organizations are often not reported to the media due to concerns over reputational damage and the potential loss of customers. Depending on the type of cybercrime, and its success, many incidents will never be reported. However, if the purpose of the successful crime was to steal the names, social security numbers, addresses, and account information, as well as credentials of customers so the records could be sold to gangs to commit identity theft, then it will undoubtedly become public. Identity theft is not the only purpose of cybercrime, but it is its most public face.

The growth of identity theft, as the fastest growing crime in America, has garnered considerable public attention and press coverage, forced the enactment of legislation at state and federal levels, and embarrassed hundreds (perhaps thousands) of publicly traded and privately held businesses, nonprofits, educational institutions, and government agencies. Angry consumers spend considerable time and money trying to straighten out damaged credit scores and deal with bill collectors for debts they did not incur. When the personally identifiable information (PII) is lost or stolen from an organization that maintained data about its' customers, donors, students, employees, veterans, taxpayers, or patients, there are serious legal, financial, and reputational ramifications. Loss of customer confidence, loss of reputation, and damage to the organization's brands can quickly ensue. Monetary costs to correct the damage can be quite expensive. For publicly traded companies, there is also a drop in share price (Rapoport, 2005).

Two kinds of incidents are responsible for a large share of the identity theft cases we hear about - phishing attacks and data breaches. Phishing works by spamming large numbers of e-mail accounts with a message, typically purporting to be from a financial institution, that there is an urgent problem with the user's account. Synovate (2007) indicates some 5% of users believe the message and click on the link in the email. They are directed to a spoofed (fake) website that looks like the one they are used to seeing for that financial institution. Once they enter their personal information, the thief will successfully collect most, maybe all, of the data needed to steal an online identity. Data breaches may expose millions of records stored in an organization's databases. Data breaches

frequently target organizations expected to yield large numbers of records. Either event can result in the loss of PII, which is frequently traded on Internet sites operated by organized criminal gangs. What the two types of incidents have in common is that phishing attacks against a company, to steal its customers' identities, may cause the customer to believe that it is the company's fault, although a spoofed website is to blame. Data breaches, with thousands or millions of records exposed, can usually be traced to a particular company, especially if the number of compromised records is sufficiently large to force public disclosure. In either case, the company will be blamed.

This paper is organized in the following sections: A description of the nature of the issue, and the extent of data breaches and identity theft, and the associated costs; a discussion of internal control frameworks used by public companies in the U.S.; application of cybercrime risk to an ERM model; and conclusions and suggestions for future work.

INDICATORS OF SCOPE AND EXTENT OF DATA BREACHES AND IDENTITY FRAUD

Identity theft is not a child of the Internet (Peretti, 2009). It is an old crime made more efficient and lucrative through the use of technology. What the Internet has done is to make possible the formation of an organized underground marketplace, with Internet chat rooms and forums, for buying or selling stolen identities and distributing the products and services needed to convert stolen PII into cash. Symantec, a provider of Internet computer security products, documented this "server economy." For 2009, the asking prices of the most-advertised pieces of a digital identity were: credit card information cost from 85 cents to thirty dollars and accounted for 19 percent of the advertisements; credentials for bank accounts also represented 19 percent of the advertisements, and were priced between \$15 and \$850 (Symantec, 2010). This server economy makes it possible to buy and sell large quantities of stolen PII.

As seen in Table 1, the incidence of identity theft fell in 2007, but increased in 2008 and again in 2009 (Javelin Research and Strategy, 2007, 2008, 2009, 2010). Amounts shown are actual amounts misappropriated and do not include any consumer costs to resolve the incidents. In many cases, these losses are being covered by banks and other institutions, so these represent increased costs of doing business on the Internet.

Table 1: Estimated Costs of Identity Theft in the U.S.

Year	No. of cases of identity theft	Fraud Losses
2006	8.4 million	\$49.3 billion
2007	8.1 million	\$45 billion
2008	9.9 million	\$48 billion
2009	11.1 million	\$54 billion

Stolen identities are worth a lot of money in the server economy, and so it is no surprise that organized criminal enterprises look for targets holding large databases of PII. The annual Verizon Data Breach Investigations Report (2010, 2009) details the actual data breaches they have investigated for their business clients. In Table 2 the numbers for 2008 and 2009 reflect the combined caseload of both Verizon and the U.S. Secret Service, which investigates financial fraud for prosecution. Note that in 2009 the average number of records exposed exceeded one million per data breach.

Table 2: Number of Breached Records, 2007-2009

Year	No. of Compromised Records	No. of Breaches
2007	171,077,984	128
2008	360,834,871	192
2009	143,643,022	141

In those cases where the party responsible for the data breach could be positively determined, the largest single perpetrator was sources external to the organization. Disturbingly, 45% of the breaches were caused by

hackers successfully penetrating computer systems' defenses. These breaches, however, accounted for 96% of the records, as shown in Table 3.

Table 3: Distribution of Breached Records by Responsible Party (2009)

Responsible party	By External Sources	By Insiders	Implicated Business Partner	Multiple Agents
No. of Records Breached	138,566,355	2,640,240	130	2,436,297
Percentage of Breaches	45%	27%	1%	27%

Costs to an organization that has suffered a data breach can be significant. In 2009, in a study of 45 organizations experiencing a data breach, expenses of a data breach averages \$6,750,000; ranging from \$750,000 to \$31,000,000 (Ponemon, 2010). Loss of stock market valuation is another aspect. An earlier study of 66 public firms that announced a "malicious" (non-accidental) Internet security breach between 1996 and 2001 found that in the two-day period subsequent to the breach, firms shed an average of 2.1 % of stock valuation, or \$1.65 billion each incident (Cavsoglu, Mishra, and Raghunathan, 2004).

Similar to the evolution of identity theft from individual perpetrators to organized crime (Peretti, 2009), the risk to organizations of a cybercrime incident is evolving, from individuals to organized crime to corporate espionage and advanced persistent threats (APTs), which are very targeted to a firm or industry and represent extreme risk. The term describes intrusions into organizations' information systems which may exist, unexposed and uninterrupted, for months. This allows an attacker to exfiltrate large amounts of data. Recent examples in 2010 have targeted Google, banks, defense contractors, chemical makers, and government agencies (McDonald, 2010). APTs appear to be aimed at stealing R&D information and other information which could be of military or economic interest to another country (Office of the Secretary of Defense, 2010). Geer (2010) defines an APT as "(a) targeted effort to obtain or change information by means that are difficult to discover, difficult to remove, and difficult to attribute." The reasons for the concern over APTs are threefold. First, the target is data, and since it is simply copied, the owner may be unaware of the loss, for long periods of time. Second, a user clicking on a link frequently is what allowed the attack software access to the firm's system. Third, the software is capable of changing and encrypting itself, such that chances of detection are diminished (Cole, 2010).

Considering the extent of cybercrime and the associated risks of loss, it would seem appropriate for an Internet-facing organization to include those risks in its risk assessment program. While applicable to many organizations, it especially applies to any company subject to the Sarbanes-Oxley Act's mandates regarding internal controls. The next section reviews the internal control frameworks most frequently mentioned in SEC regulatory filings.

CONTROL FRAMEWORKS FOR ASSESSING INTERNAL CONTROLS OVER FINANCIAL REPORTING

Perhaps the most contentious issue that the passage of the Sarbanes Oxley Act of 2002 caused was the required management assessment and auditor certification of the effectiveness of a SEC registrant's internal controls over financial reporting (ICFR). As part of management's report, it must name the recognized framework it used to assess the internal control system.

While there are a number of frameworks available internationally, this review focuses on those most frequently mentioned in U.S. regulatory filings:

- Control Objectives for Information and Related Technology (COBIT, 2005)
- COSO's Internal Control – Integrated Framework (1992)
- COSO's Enterprise Risk Management – Integrated Framework (2004)
- COSO's Guidance for Smaller Public Companies (2006)

For purposes of evaluating the internal control system, the SEC requires the use of a recognized control framework, and the PCAOB Auditing Standard No. 5, “An Audit of Internal Controls Over Financial Reporting That is Integrated With an Audit of Financial Statements” requires that an auditor use the same framework as did management in its review. A search of *Compliance Week* showed thousands of public companies use the 1992 framework. An apparently much smaller number use the Enterprise Risk Management framework, and a number reported using the 1992 framework in conjunction with the COBIT model. Hundreds of firms reported using the Guidance for Smaller Public Companies. A number of companies have developed or purchased enterprise risk management systems.

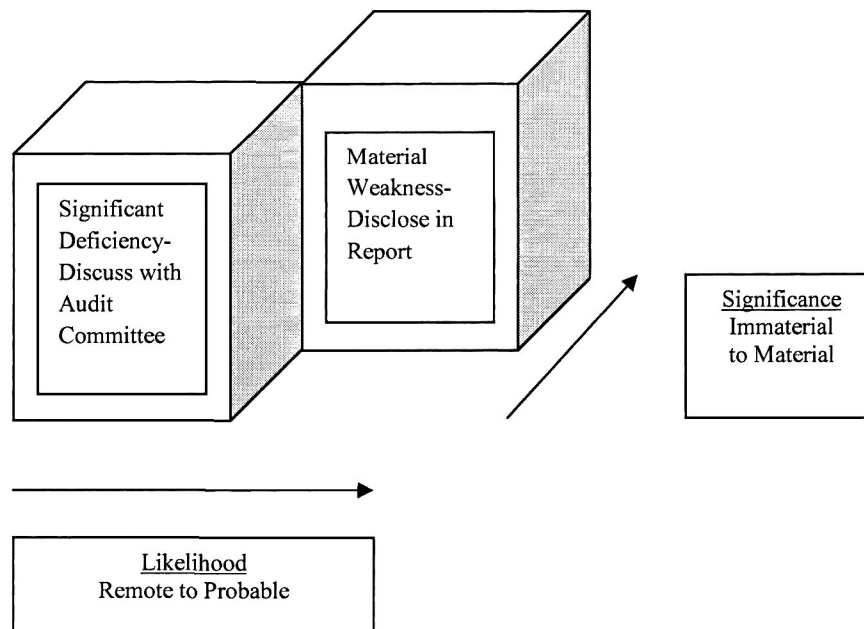
These frameworks serve as benchmarks against which a company can evaluate its control policies and procedures. They are differentiated as follows:

- Control Objectives for Information and Related Technology (COBIT). For guidance on controlling information technology many organizations rely on the COBIT framework. COBIT is a product of ISACA, formerly Information Systems Audit and Control Association. COBIT was first released in 1996, with the fourth version released in 2005. COBIT considers life-cycle control of IT systems and related technologies. For this reason some public companies report using the 1992 COSO guidance, supplemented by COBIT.
- COSO’s Internal Control – Integrated Framework. The Committee of the Sponsoring Organizations of the Treadway Commission issued the first guidance on internal control to provide some uniformity to the design of internal controls for the accounting and auditing community in 1992. This is widely used by public companies. It is focused on internal controls from a management perspective, and does not have the risk assessment features of its successor.
- COSO’s Enterprise Risk Management – Integrated Framework. In 2004 COSO issued the Enterprise Risk Management – Integrated Framework to expand on internal control and provide a perspective on enterprise-wide risk management.
- COSO’s Internal Control over Financial Reporting – Guidance for Smaller Public Companies (2006) did not modify the original 1992 framework, but is aimed at smaller companies to help them design, implement and maintain internal control in cost-effective fashion. A set of illustrative assessment tools is included.

And the guidance is still needed, six years after Sarbanes-Oxley became effective. To illustrate, a search of *Compliance Week* for the first six months of 2010 revealed 290 unique firms reporting ineffective internal controls resulting in one or more material weaknesses in their internal controls over financial reporting.

The Sarbanes-Oxley Act (SOX) of 2002, Section 302, requires public companies’ management to attest to the adequacy of internal controls over financial reporting. Section 404 requires the companies’ auditors to attest to and report on management’s assessment of internal controls. Under Section 302, management is responsible for establishing, maintaining, and regularly evaluating the effectiveness of its internal controls over financial reporting. If deficiencies are found, they must be evaluated in two dimensions, significance and likelihood, to identify their relative significance (see Figure 1). The evaluation of internal control deficiencies must consider whether the internal control system is incapable of stopping material errors from entering the financial statements. This requires considering the likelihood of that happening (from remote to probable) and the significance of a potential misstatement (from immaterial to material). As Figure 1 indicates, those deficiencies that have a more than remote likelihood of occurring will have to be disclosed in the opinion, if they are judged to be material. Those significant deficiencies that do not rise to the level of a material weakness will not be reported out but need to be discussed with the audit committee.

Figure 1: Disclosure of Internal Control Deficiencies



Adapted from Ramos (2004)

APPLICATION OF CYBERCRIME RISK TO AN ERM FRAMEWORK

In the U.S., enterprise risk management is not as widely adopted as it is elsewhere. Beasley, Branson and Hancock (2010) report that

"46% of global respondents describe their risk oversight process as systematic, robust, and repeatable in contrast to 11% of U.S. respondents who believe they have a complete enterprise-wide risk management process in place." (p. 4)

Their findings are supported in this paper. As noted earlier the majority of companies appear to still be using the original COSO framework, and there continue to be hundreds of firms annually forced to report their ICFR were ineffective. If there are that number of ineffective ICFRs in public firms using the oldest framework, one must consider whether there are additional risks to ICFR which are not being examined. Upgrading their framework to an enterprise-wide risk management model would provide an opportunity to unlock value, by looking at risk and opportunity across the firm's units. Below is brief overview of the COSO ERM model, followed by a description suggesting how this could be implemented using the COSO ERM framework to include cybercrime risks.

In 2004, COSO issued the Enterprise Risk Management – Integrated Framework (ERM), incorporating the previous internal control focus within a risk management view of the enterprise:

"Enterprise Risk Management (ERM) is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (COSO, 2004)

This approach allows management to avail itself of opportunities, so long as the risks are understood and the returns are acceptable.

The COSO framework provides the most comprehensive tool yet for organizations to identify possible risks, assess the effects of particular risks on the organization, and find ways to manage the risks. The document provides four categories of objectives that help organizations meet their goals:

1. Strategic - High-level goals, aligned with and supporting its mission.
2. Operation – Effective and efficient use of its resources.
3. Reporting – Reliability of reporting.
4. Compliance – Compliance with applicable laws and regulations.

Enterprise risk management, as envisioned by COSO, is a product of the way a company is operated. As a structure for understanding risk, there are eight components that consider internal and external agents and events (see Table 4). In the context of a risk management plan that incorporates cybercrime risk, COSO's ERM model has provisions for that risk. The three relevant (shaded) components are Event Identification, Risk Assessment, and Risk Response.

Table 4: COSO ERM Internal Controls Components

Component	Description
Internal Environment	<ul style="list-style-type: none"> • Tone of the organization. • Risk Management Philosophy. • Risk Appetite. • Board of Directors. • Integrity, ethical values, and competence. • Organizational structure. • Assignment of authority and responsibility. • Human resource standards.
Objective Setting	<ul style="list-style-type: none"> • Strategic objectives. • Operational objectives. • Reporting objectives. • Compliance objectives. • Risk appetite and tolerances.
Event Identification	<ul style="list-style-type: none"> • Events that affect strategy or objectives. • External factors – economic, natural environment, political, social, and technological. • Internal factors – infrastructure, personnel, process, and technology. • Identification techniques.
Risk Assessment	<ul style="list-style-type: none"> • Inherent and residual risk. • Estimating likelihood and impact. • Assessment techniques.
Risk Response	<ul style="list-style-type: none"> • Response choices: avoid, reduce, share, or accept. • Portfolio view.
Control Activities	<ul style="list-style-type: none"> • Relation to strategic, operations, reporting and compliance objectives. • Integrated with risk responses. • Types of control activities. • Policies and procedures. • Controls over information systems.
Information & Communication	<ul style="list-style-type: none"> • Systems integrated with outside parties. • Technology choices affect meeting objectives. • Reliance on systems to achieve strategic and operating objectives increases risks of security breaches and cybercrimes. • Communication: Internal; external.
Monitoring	<ul style="list-style-type: none"> • Ongoing monitoring activities. • Separate evaluations.

EVENT IDENTIFICATION PROCESS

COSO suggests five broad “event categories” as a starting point for identifying threats and opportunities: Economic, Natural environment, Political, Social, and Technological. As Table 5 indicates, cybercrimes like

phishing attacks and externally-sourced data breaches, may impact an organization in all categories, except for natural disasters. For the remaining four event categories, there are one or more factors external to the organization that may present a threat. Included with the threats are the risks that the threat presents.

Table 5: External Factors and Identity Theft Risk

Event Category	External Factor	Examples of Threats & Risks
Social	Privacy; Consumer Behavior;	Targeted phishing attack leads to customers' personal information being sold to criminals, used for identity theft. <ul style="list-style-type: none"> • Lawsuits, damages. • Loss of customers. • Negative publicity. • Public notification laws may require disclosure.
	Terrorism; Server Economy	Organized crime gang conducts large-scale theft of customers' personal information for identity theft purposes, through a data breach. <ul style="list-style-type: none"> • Lawsuits, damages. • Loss of customers. • Negative publicity. • Public notification laws may require disclosure. • May be forced to submit to outside security audits for years. <p>Existence of an organized marketplace for identity data.</p> <ul style="list-style-type: none"> • Increased demand for stolen personal data. • Targets will be whichever websites or computers are most vulnerable.
Technological	Electronic Commerce;	If business is only online, business model at risk. <ul style="list-style-type: none"> • All parts of an e-business are on the server. • Identity theft of customers, donors, or other stakeholders. • Theft of money / goods. • Customer list compromised.
	Emerging Technology	New technology is introduced which defeats previous internal controls. <ul style="list-style-type: none"> • Wireless networks. • In-session pop-up windows. • Advanced persistent threats.
Economic	Mergers & Acquisitions;	Poor due diligence on target/partner's information systems internal controls. <ul style="list-style-type: none"> • Poor understanding of partner's inventory of sensitive personal data. • Lack of policy & controls over partner's access to/use of your customer accounts.
	Business Partners; Outsourcing	<ul style="list-style-type: none"> • Overseas vendors difficult to sue. • Need for SAS 70 data center audits. • Poor controls at vendor.
Political	Legislation; Regulation; Public Policy	State and federal legislatures will enact restrictive or costly legislation with different provisions. <ul style="list-style-type: none"> • Expansion to a new state /nation entails review of existing controls to conform with that body's rules.

RISK ASSESSMENT PROCESS

Proceeding from the event inventory developed in Table 5, we can move to the next component - risk assessment. Here we consider both inherent and residual risk. Inherent risk is the amount of risk existing if management takes no steps to limit it. The remaining risk, after management develops a response is the residual risk. Table 6 is a hypothetical example of an assessment of whether certain events that might lead to identity theft could occur, and what the likelihood of occurrence is. COSO suggests some time frame might be set, say for the next 18 months. This helps to limit the analysis to the near-term, and is a means of establishing this as a periodic exercise, not a one-time event.

Table 6: Risk Assessment for Identity Theft

Descriptor	Likelihood of Occurrence	Risk
Possible	Moderate	Customer identity theft results from a phishing attack.
Unlikely	Low	Customer identity theft results from a data breach.
Likely	High	New legislation will require revised or new internal controls.
Possible	Moderate	Wireless networks will be installed with poor controls.

RISK RESPONSE PROCESS

Once the risk assessment is completed, management can consider its options for dealing with the risks. In COSO's model, there are four choices - avoidance, reduction, sharing, and acceptance. Table 7 suggests some possibilities in each of these categories for an organization concerned about identity theft or other forms of cybercrime.

Table 7: Possible Risk Responses for Identity Theft Risks

Risk Avoidance	Risk Reduction
<ul style="list-style-type: none"> • Redesign information needs to avoid collecting as much personal data as possible. • Discontinue/sell the business line that requires personal data. 	<p>Website</p> <ul style="list-style-type: none"> • Contract with a website monitoring service. • Purchase similar domain names. • Register website with a security vendor. • Contract with a domain hosting service. <p>Data Inventory</p> <ul style="list-style-type: none"> • Review data retention policy. • Create a data destruction schedule. • Inventory of storage locations of sensitive data. • Policy on sales of old storage media. <p>Management</p> <ul style="list-style-type: none"> • Contingency plan. • Manage customer password changes. • Someone in charge. <p>Vendors, Employees</p> <ul style="list-style-type: none"> • Review relationships with data brokers. • Vendors audited for security; data center audits. • Background checks.
Risk Sharing	Risk Acceptance
<ul style="list-style-type: none"> • Contract agreements with vendors, customers, partners. • Outsourcing limited to US - located vendors. • Purchase cyber insurance. • Offer identity theft insurance. 	<ul style="list-style-type: none"> • Accept the risk as being within the organization's risk tolerance. • Self-insure.

CONCLUSIONS

If one or more of the events described were to occur, there is the possibility that it would affect the organization's accomplishment of both operating and compliance objectives.

Under the Event Identification component, phishing attacks and data breaches are a common enough problem that they should be included as an event that would, if successful, pose a risk to the company. If identified as a risk-causing event, then the development of an appropriate risk assessment and risk response would be required.

Phishing and other forms of electronic attack would clearly have an adverse affect on both operational and compliance objectives. Operational objectives, such as profitability, may be affected by the costs of fighting and shutting down a phishing site. Since a phishing attack works by highjacking a known and trusted brand name, the objective of safeguarding resources/assets, including the brand, is compromised.

Privacy is always an issue when online identities are stolen. If enough records are compromised, the attack could result in a public notification of the fact (depending on which state the organization is in). Terrorism, in an electronic form, can be as simple as a denial of service attack against a company or government agency or internet service provider.

Loss of proprietary data, such as marketing plans, R&D work, merger and acquisition due diligence reports, or other information of value to an organization, may be lost if the firm's information systems are attacked. Many firms that suffer these kinds of losses are unaware that external sources have planted software on their systems, sometimes for many months. This allows for large quantities of data to be stolen over time.

Technological risks include risks to electronic commerce and emerging technology. As soon as a company opens its web site, it becomes exposed to global threats. Increased dependency on the website (i.e., for a share of sales) exposes the company to these risks. Emerging technologies may represent a possible new threat or a change in an existing one. For example, the new pop-up phishing window that opens while a customer is in an online banking session. In this much more targeted attack (all customers are clients of the bank being spoofed), a window opens, telling the customer her session has timed out, and she needs to re-enter her user name and password. Once that data has been harvested, the customer is passed back to the real bank site.

Ge and McVay (2005) presented a plan for classifying material weaknesses that contained nine types of material weaknesses. Below, based on that, are five types of material weaknesses that could be associated with cybercrime risk:

1. Senior management (allowing an ineffective internal control environment): A management team that is unfamiliar with online threats may not understand when additional resources, such as either more experienced staff or a security monitoring firm are needed.
2. Training (inadequate training or staffing such that effective and timely reviews are not performed): Numerous phishing attacks and data breaches go undetected for weeks and even months because reviews of computer security are not performed or not done well enough to detect the problem. Examples of this include not reading system log files to check for the installation of unauthorized software and not testing the data being sent out from the system for unusual amounts.
3. Technology issues (for an E-commerce business, all parts of the business are on the server): Consumer fears over security of their PII or denial of service attacks could impair the business sufficiently to raise going concern issues.
4. Account-Specific: Any identity theft that may require reimbursement of customers' losses or the provision of credit-monitoring services represents a future liability, so liabilities would be understated.
5. Account-Specific (attacks that may lead to the loss of intellectual property): If the asset were purchased, impairment issues could arise, with the effect the asset was overvalued on the financial statements.
6. Accounting policies (lack of control over business partner's use of organizational information assets): Business partners' or contractors controls over information may lead to loss or misappropriation of data.

SUGGESTIONS FOR FUTURE RESEARCH

As cybercrime evolves, more organizations will likely fall victim, and this may lead to larger numbers of ERM adoptions. If governments and large public firms continue to go public about advanced persistent threats, this, too, could drive more firms to include these threats in their risk assessments. The following are suggested for future research. A comparison of firms using the original 1992 COSO model versus firms using an ERM model, based on the number and type of reported weaknesses, could be instructive in terms of identifying industries and attributes leading to ERM adoption. On the security side a comparison of information security budgets might lead to a model budget; evaluation of the incidence of outsourcing of the information security function could lead to an understanding of what works and what doesn't.

AUTHOR INFORMATION

John W. Moore earned his Ph.D. at Virginia Commonwealth University. He is a (Virginia) CPA. Current research interests include research and development funding and productivity, and internal control systems for public firms.

REFERENCES

1. Beasley, Mark S., Branson, Bruce C. and Hancock, Bonnie V., 2010. Enterprise risk oversight A global analysis. CIMA and AICPA research series. The ERM Initiative at North Carolina State University, www.erm.ncsu.edu
2. Cavsoglu, Huseyin, Mishra, Birendra, and Raghunathan, Srinivasan, 2004. The Effect of Internet Security Breach on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, Fall 2004, Vol. 9, No. 1, pp. 69-104.
3. Cole, Eric. 2010. Advanced Persistent Threat (APT). McAfee Security Insights Blog. <http://siblog.mcafee.com/cto/advanced-persistent-threat-apt/>
4. Committee of Sponsoring Organizations, 2004. Enterprise Risk Management-Integrated Framework, Executive Summary. New York: The Committee of Sponsoring Organizations of the Treadway Commission, 2004.
5. _____, 2006. Internal Control over Financial Reporting – Guidance for Smaller Public Companies. New York: The Committee of Sponsoring Organizations of the Treadway Commission, 2006.
6. Ge, Weili and McVay, Sarah. 2005. The disclosure of material weaknesses in internal control after the Sarbanes- Oxley Act. *Accounting Horizons* 19(3): 137-158.
7. Geer, Daniel. 2010. Advanced Persistent Threat. Network World April 12, 2010. <http://www.networkworld.com/news/tech/2010/041210-tech-update.html>
8. Javelin Research and Strategy. 2007. <http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study>.
9. Mills, Elinor, 2009. Payment Processor Heartland reports breach. Cnet news, January 20, 2009. http://news.cnet.com/8301-1009_3-10146275-83.htm
10. McDonald, Joe, 2010. Google charge highlights China-based hacking. Msnbc.com, Feb. 3, 2010. http://www.msnbc.msn.com/id/35222681/ns/technology_and_science-security.
11. Office of the Secretary of Defense, 2010. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China. www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf
12. Peretti, Kimberly Kiefer. 2009. Data Breaches: What the Underground World of “Carding” Reveals. *Santa Clara Computer & High Tech Learning Journal*. Vol. 25, pp376-413.
13. Ponemon Institute LLC, 2010. 2009 Annual Study: Cost of a Data Breach. [www.http://ponemon.org/localupload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf](http://www.ponemon.org/localupload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf)
14. Ramos, Michael, 2004. Section 404 Compliance in the Annual Report. *Journal of Accountancy*. New York: Oct. 2004. Vol. 198, Issue 4, pp 43-47.
15. Rapoport, Michael, 2005. Companies Pay a Price For Security Breaches; In Most Cases, Shares Fall Moderately After Disclosure And Then Can Stay Down. *Wall Street Journal (eastern Edition)* June 15, 2005: (C3).
16. Symantec Corporation. 2010. *Symantec Global Internet Security Threat Report – Trends for 2009*. Vol. XV, April 2010.
17. Synovate, 2007. Federal Trade Commission – 2006 Identity Theft Survey Report. <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.
18. Verizon Business. 2009. 2009 Data Breach Investigations Report. http://www.verizonbusiness.com/resources/security/reports/2009_databreaches_rp.pdf
19. Verizon Business. 2010. 2010 Data Breach Investigations Report. http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf